REMARKS

This amendment is being filed in response to an Office Action mailed 01/13/2005, in which the Examiner said that claims 1-25 were pending but rejected. In this amendment, claims 1 and 13 are amended, and various grounds for rejection are traversed below.

Claim 1 is amended to remove the hyphen from "computer-readable" to provide an antecedent basis compatible with subsequent usage of the term in the claims.

Claims Rejected under 35 USC §112

In the Office Action, the Examiner said that claims 13-18 were rejected under 35 USC §112, second paragraph, as being indefinite, since claim 13 recites the limitation "said removable computer readable medium" in line 4, for which there was insufficient antecedent basis.

In this amendment, this limitation of claim 13 is modified to read "said computer readable medium," for which antecedent basis is found in line 2 of the same claim. It is understood that claims 14-18 were rejected under 35 USC §112, second paragraph, because of their dependence upon claim 13, so that the rejection of these additional claims is overcome by the modification of claim 13. The Applicants respectfully submit that the claims now meet the requirements of 35 USC §112, second paragraph. Reconsideration and withdrawal of this reason for rejection is respectfully requested.

Claims Rejected under 35 USC §103

The Examiner additionally said that claims 1-7 and 11-24 were rejected under 35 USC §103(a) as being unpatentable over U.S. Pat. No. 6,832,316 to Sibert, in view of U.S. Pat. No. 6,463,537 to Tello, and further in view of U.S. Pat. No.

6,507,911 to Langford.

The Applicants' invention provides a method for securing a large amount of data, stored within a hard disk drive medium or on a removable computer readable medium, by encrypting a small amount of data within a data structure including information locating the various data records on the medium. This method avoids a need to encrypt and subsequently decrypt all of the data to be protected. On the other hand t, the method of Sibert requires that all of the data to be protected is encrypted and subsequently decrypted (see, for example, column 3, lines 8-12, 20-23, column 5, lines 12-17).

Regarding claim 1, the Examiner further indicated that Sibert described a method for decrypting said encrypted version of said first data structure to form said first data structure in column 6, lines 55-67. However, as described in claim 1 of the Applicants' invention, "said data structure" must be the "first data structure," which locates data records in the plurality of data records stored on the computer readable medium. On the other hand, Sibert describes, in column 6, lines 55-67, an embodiment in which decoding logic is used at system start-up to decrypt and validate system control programs to be operable to initialize and control the operation of the system 42. The system 42 can then be used to decrypt data. There is no indication that the data itself is decrypted in the method of Sibert at system start-up, or that it is even available for decryption at that time. There is no indication that the system of Sibert decrypts a data structure locating data records within the data at that time or at any other time.

The Examiner additionally indicated that Sibert discussed a method for encrypting in column 5, lines 41-67. However, Sibert describes, in column 5, lines 40-44, a system including an encoding system, such as a computer, for encoding messages or data and transmitting the resulting ciphertext to a recipient's system. Then, in column 6, lines 22-24, the recipient's system is

operable to decode and validate the encoded data. Thus, all of the data to be protected---in this case, the data being transmitted---is encrypted and subsequently decrypted. There is no indication that a data structure locating data records within the data to be protected is encrypted and then decrypted.

As further indicated by the Examiner, Tello teaches performing tasks at shut down. However, as described in the Abstract, Tello teaches that selected data storage devices and other user selectable devices should be enabled and disabled at system start-up and shut-down, not that a data structure locating data records should be decrypted and encrypted at these times.

As additionally indicated by the Examiner, Langford teaches deleting data that has been encrypted and replacing it with an encrypted version of the data. However, Langford does not anticipate that the data being encrypted and deleted includes a data structure indicating the locations of records within data to be protected.

For all of the reasons discussed above, the Applicants respectfully submit that Sibert, Tello, and Langford, taken separately or in combination, fail to describe, teach, or otherwise anticipate the requirements of claim 1 for the encryption subroutine to read a first data structure from the computer readable medium, to produce an encrypted version of the first data structure, to delete the first data structure from the computer readable medium, and to store the encrypted version of the first data structure, *wherein the first data structure locates data records in a plurality of data records stored on the computer readable medium.* Furthermore, for all of the reasons discussed above, the Applicants respectfully submit that Sibert, Tello, and Langford, taken separately or in combination, fail to describe, teach, or otherwise anticipate the requirements of claim 1 for the decryption subroutine to read the encrypted version of the first data structure from the nonvolatile storage, to decrypt the encrypted version of the first data structure, to

delete the first data structure from the computer readable medium, and to write the data structure to the computer readable medium, *wherein the first data structure locates data records in a plurality of data records stored on the computer readable medium.*

Furthermore, the Applicants respectfully submit that the references cited by the Examiner teach against these requirements of claim 1, with Sibert teaching that the entirety of the data to be protected should be encrypted and subsequently decrypted, and with Tello teaching that security should be achieved by enabling and disabling peripheral devices at system start up and shut down.

For all the above reasons, the Applicants respectfully submit that claim 1 is patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford.

Regarding claims 2, 3, 5-7, 11, and 12 since these dependent claims merely add limitations to claim 1, the Applicants respectfully submit that, for reasons described above regarding claim 1, claims 2, 3, 5-7, 11 and 12 are patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford.

Regarding claim 4, the Applicants respectfully submit that Langford clearly teaches that encrypted data should be recorded in the location on the computer readable medium from which the unencrypted version of the data is deleted, not that such encrypted data should be stored in a location within non-volatile storage separate from the computer readable medium, as required by claim 4. Tello teaches enabling and disabling peripheral devices instead of the storage of encrypted data in a location separate from the computer readable medium.

The Examiner has cited Sibert, column 6, lines 55-67, in regard to this claim.

However, as described above regarding the rejection of claim 1, this portion of Sibert describes the decryption of system control programs, not of a data structure locating data records in data to be secured.

For the above reasons, and additionally since claim 4 merely adds limitations to claim 1, for reasons described above regarding claim 1, the Applicants respectfully submit that claim 4 is patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford.

Regarding claims 13 and 19, as described in detail above regarding the rejection of claim 1, Sibert, Tello, and Langford do not describe the encryption and subsequent decryption of a data structure describing the locations of data records on the computer readable medium being protected, with Sibert instead teaching that the entirety of the data to be protected should be encrypted and decrypted, and with Tello teaching that peripheral devices should be enabled and disabled at system start up and shut down.

Therefore, the Applicants respectfully submit that Sibert, Tello, and Langford, taken separately or in combination, fail to describe, teach, or otherwise anticipate the requirements of claim 13 for the encryption subroutine to encrypt said first data structure and for a decryption subroutine subsequently executed to decrypt said encrypted version of said first data structure, and for these encryption and decryption processes to within a cryptographic processor, *wherein said first data structure locates data records in a plurality of data records stored on a computer readable medium.*

In addition, for reasons described above, the Applicants respectfully submit that Sibert, Tello, and Langford, taken separately or in combination, fail to describe, teach, or otherwise anticipate the requirements of claim 19 for a microprocessor to be programmed to execute a data structure encryption routine to encrypt said

first data structure and to execute subsequently data structure decryption routine to decrypt an encrypted version of said first data structure, *wherein said first data structure provides locations and sequences for accessing data within said data records.*

Therefore, the Applicants respectfully submit that claims 13 and 19 are patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford.

Regarding claim 14, the Applicants respectfully submit that Sibert, Tello, and Langford, taken separately or in combination, fail to describe, teach, or otherwise anticipate the requirement of claim 14 for the encryption program to be executed in response to receiving a request to shut down the computing system and for the encryption routine to be executed in response to electrical power being turned on within the computing system. Langford does not describe encryption and decryption occurring in response to the system being shut down or turned on. Tello describes peripheral devices being disabled and enabled as the system is shut down or turned on. Sibert describes system control programs, not a data structure locating data records, being decrypted when the system is turned on. There is no indication that the control programs are encrypted when the system is turned off; they may be stored in an encrypted form whether or not the system is running.

Therefore, and additionally because claim 14 merely adds these limitations to claim 13, which is believed to be patentable for reasons described above, the Applicants respectfully submit that claim 14 is patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford.

Regarding claims 15-18, the Applicants respectfully submit that, since these claims merely add limitations to claim 13, for reasons described above regarding

claim 13, claims 15-18 are patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford.

Regarding claims 20-24, the Applicants respectfully submit that, since these claims merely add limitations to claim 19, for reasons described above regarding claim 19, claims 20-24 are patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford.

Regarding claims 8, 9, and 25, the Examiner indicated that these claims were rejected under 33 USC §103(a) as being unpatentable over a modified Sibert, Tello, and Langford system, further in view of U.S. Pat. No. 5,544,356 to Robinson et al., with Robinson et al. teaching a boot record describing the file allocation table. Nevertheless, the Applicants respectfully submit that adding the teachings of Robinson et al does not provide a description of the encryption and subsequent decryption of a data structure locating various data records, with such a description being missing from the disclosure of the other cited patents. Therefore, and additionally because claims 8 and 9 merely add limitations to claim 1, and further because claim 25 merely adds limitations to claim 19, the Applicants respectfully submit that claims 8, 10, and 25 are patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford and additionally in view of Robinson et al.

Regarding claims 8, 10, and 25, the Examiner indicated that these claims were rejected under 33 USC §103(a) as being unpatentable over a modified Sibert, Tello, and Langford system, further in view of U.S. Pat. No. 6,070,174 to Starek et al., with Starek et al. describing an array of file records in a master file table of an NTFS file, and a second data structure including metafile data in the master file table. Nevertheless, the Applicants respectfully submit that adding the teachings of Starek et al does not provide a description of the encryption and subsequent decryption of a data structure locating various data records, with

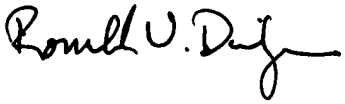
such a description being missing from the disclosure of the other cited patents. Therefore, and additionally because claims 8 and 10 merely add limitations to claim 1, and further because claim 25 merely adds limitations to claim 19, the Applicants respectfully submit that claims 8, 10, and 25 are patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford and additionally in view of Starek et al.

Regarding claims 1-25, the Examiner additionally indicated that claims 1-25 were rejected as previously described but in view of JP2001202167A, which discloses a control method for a computer, involving the encrypting and decoding data in memory based on power on or off in the power supply. However, the Applicants respectfully submit that this Japanese patent teaches that the entire contents of the memory should be encrypted and decrypted. Again, there is no teaching of the encryption and decryption only of a data structure describing the location of data records to be protected. Therefore, the Applicants respectfully submit that claims 1-25 are patentable under 35 USC §103(a) as described above and further in view of JP2001202167A.

Conclusions

The Applicants respectfully submit that the application, including claims 1-25, is now in condition for allowance, and that action is earnestly requested, with reconsideration and withdrawal of all reasons given for rejections.

Respectfully submitted,



Ronald V. Davidge
Registration No. 33,863
Telephone No. 954-344-9880